(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 January 2005 (20.01.2005)

PCT

(10) International Publication Number
WO 2005/006703 A2

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number: PCT/EP2004/050864

(22) International Filing Date: 19 May 2004 (19.05.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
03102111.6 11 July 2003 (11.07.2003) EP

(71) Applicant *(for all designated States except US)*: **INTERNATIONAL BUSINESS MACHINES CORPORATION** [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **HAGMEIER, Joachim** [DE/DE]; Forststr. 93, 70176 Stuttgart (DE). **BRUCHLOS, Joachim** [DE/DE]; Hirsauer Wiesenweg 45, 75365 Calw (DE). **KUSSMAUL, Timo** [DE/DE]; Furtwanger Str. 14, 71034 Boeblingen (DE).

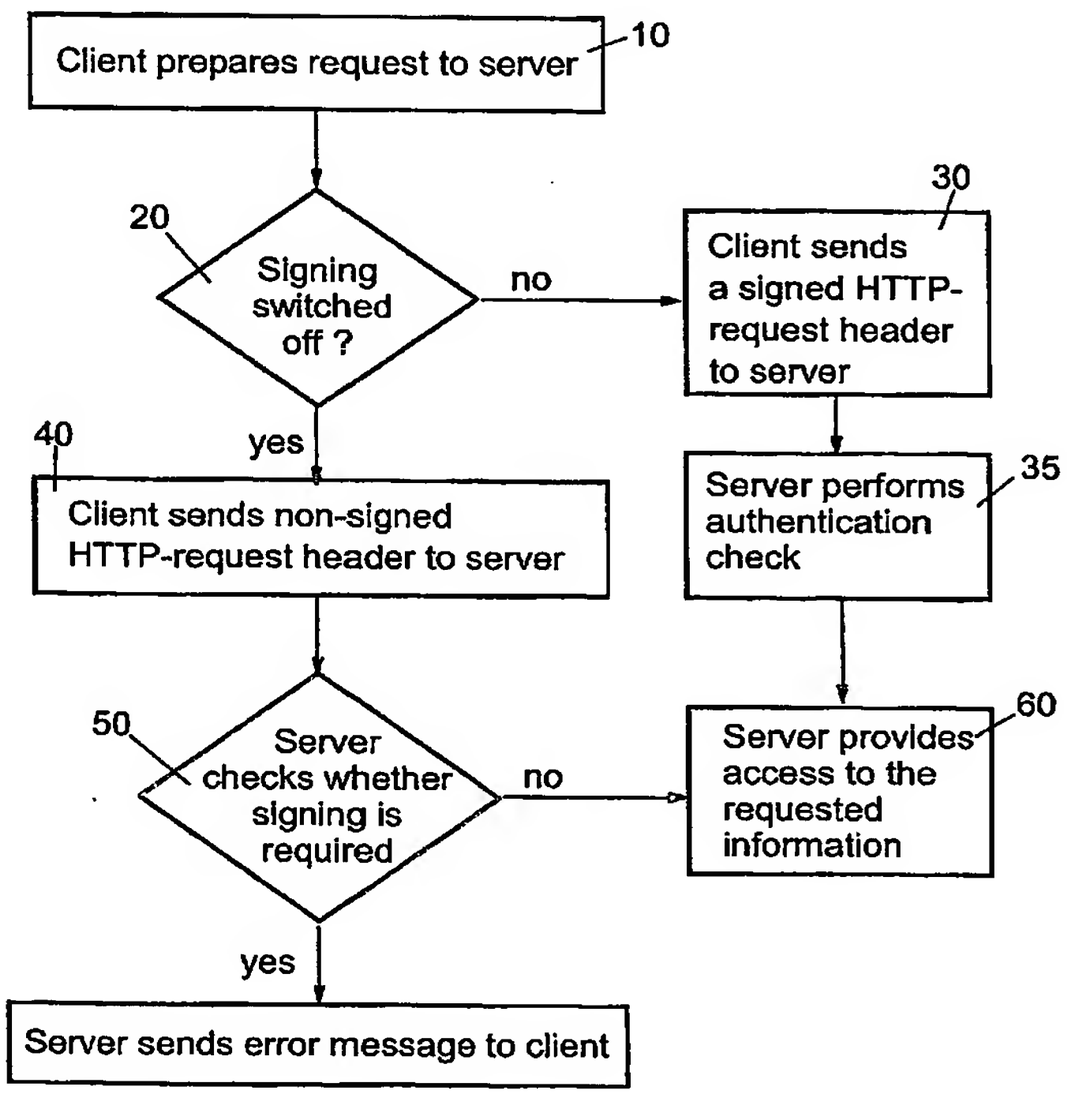
(74) Agent: **KLEIN, Hans-Jörg**; Postal Code, 70548 Stuttgart (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

*[Continued on next page]*

(54) Title: SYSTEM AND METHOD FOR AUTHENTICATING CLIENTS IN A CLIENT-SERVER ENVIRONMENT




(57) Abstract: The idea of the present invention is to replace the existing password/user ID based authentication process by a new digital signature authentication process in which preferably the first HTTP-request header is extended by the client authentication information independently of the authentication process used by the destination server and without server requesting authentication information. The authentication information preferably includes the client certificate containing the client public key, signed by certification authority, and preferably a hash value calculated over the HTTP-request header data being sent in the request, and encrypted with the Client's private key. The certificate and digital signature may be added during the creation of the HTTP-request header in the client system itself, or may be added later in a server acting as a gateway, proxy, or tunnel. A destination server that does not support the new digital signature authentication process will simply ignore the certificate and digital signature in the HTTP-request header and will automatically initiate its own authentication process. The present invention simplifies the existing digital signature authentication process and concurrently allows the coexistence of different authentication processes without changing the HTTP-protocol or causing unnecessary network traffic.

WO 2005/006703 A2

**Published:**

— *without international search report and to be republished upon receipt of that report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*